



FlexNet Publisher 2016 R1 Service Pack 2 (11.14.0.2)

Revision 0 – last updated 10 October 2016

Table of Contents

Resolved Items in Service Pack 2	2
Solaris Platforms Included in Service Pack 2.....	2
PACKAGE, SUITE_DUP_GROUP and borrow	2
Server periodic check for VDH	2
FreeBSD License Server Connection Limit	2
First-Checkout Performance Improvement on Windows.....	2
AMZN_EIP Server HostID	2
Error code displayed when the FNLS is older than the FNP client.....	2
Resolved Items in Service Pack 1	3
The FlexNet Licensing Service, Virtualization and Performance Improvements	3
Other Virtualization Resolved Issues	4
Other FlexNet Licensing Service issues	5
Certificate borrow resolved issues	5
Windows Visual Studio 2015 compatibility	5
Dongle updates	6
3-Server enhancement	6
VCG enhancement.....	6
Resolved certificate issues	7
Java kit resolved issue.....	7
Lmadmin resolved issues	7
Trusted Storage resolved issues.....	9
Supported Platforms.....	10
Legal Information.....	10

Resolved Items in Service Pack 2

Note: Service Pack 2 is cumulative to Service Pack 1; Imadmin is not updated in Service Pack 2.

Solaris Platforms Included in Service Pack 2

FlexNet Publisher Solaris platforms were not included in 11.14.0.1, but are included in 11.14.0.2 (FNP-15231).

PACKAGE, SUITE_DUP_GROUP and borrow

Previously, when borrowing two features with checkout data and the features specified as components of a package where SUITE or SUITE_RESERVED with DUP_GROUP, two counts of the parent package were incorrectly consumed instead of one. This has been resolved. The fix affects only the vendor daemon (FNP-15183).

Server periodic check for VDH or VM_UUID

Previously, when running on a virtual machine, the vendor daemon would not perform a periodic check for the vendor-defined hostid (VDH) or the VM_UUID, when using one of these as the SERVER line HostID. This has been resolved (FNP-15182).

FreeBSD License Server Connection Limit

Previously, a FreeBSD vendor daemon would not support more than (approximately) one thousand client connections. Now, up to ten thousand client connections are supported, with a theoretical maximum of approximately sixty-five thousand connections (FNP-15089).

Note: FreeBSD is a limited availability and a functional-restricted platform.

First-Checkout Performance Improvement on Windows

In 11.14.0.1 the first-checkout performance was improved but only for the case where the FlexNet Licensing Service (FNLS) was installed. Since certificate-only customers do not typically install the FNLS, this service pack delivers the same performance improvement when the FNLS is not installed (FNP-15370). Refer [below](#) for the limitations on virtualization behaviour when FNLS is not installed

AMZN_EIP Server HostID

Previously, using AMZN_EIP as a SERVER line HostID could cause a restart when a server reread is performed. This instability issue is resolved (FNP-15137).

Error code displayed when the FNLS is older than the FNP client

In 11.14.0.1 a bug was introduced where a system error code was not returned when the FNLS was older than the Windows FNP client. In 11.14.0.2, system error LM_TSSE_SERVICE_TOO_OLD is now returned, once again (FNP-15034).

Resolved Items in Service Pack 1

The FlexNet Licensing Service, Virtualization and Performance Improvements

Virtualization detection has previously been performed at the time of the first checkout against a job. As virtualization detection techniques have been incrementally added across FlexNet Publisher (FNP) releases, this has resulted in a cumulative performance degradation for first-time checkout latency for a job (FNP-14829). Similar latencies will have occurred across activation APIs which indirectly or directly query a system's virtualization attributes, such as `flxActCommonHandleGetUniqueMachineNumber` when used to extract UMN3.

Consequently, the design change is to have all virtualization attributes extracted and cached via the FlexNet Licensing Service (FNLS). Whilst this change is limited to Windows in 11.14.0.1, the next major release of FNP will deliver this change for Linux platforms.

Since the design change requires the FNLS to regularly poll the system to update virtualization data, the FNLS now runs continuously, whereas previously it would shut down after a period of not being used. The virtualization poll interval is not configurable, and Flexera Software reserves the right to change it in the future.

Best practice for the FNLS is now for it to be started automatically on OS boot, so that virtualization attribute extraction is complete ahead of a first-checkout, ensuring a performant licensing experience. The `installanchorservice` utility now implements this best-practice.

Certificate-only applications have historically not needed to install the FNLS. Whilst good reasons for installing the FNLS even for certificate-only applications accumulate (it is for example needed for the vendor daemon VM Generation ID nag message feature) the FNLS is still unnecessary for certificate-only applications *that do not use virtualization features*. Therefore, in Windows certificate-only applications, installing the FNLS effectively becomes a switch for enabling virtualization detection.

Note: Future versions of FNP are likely to add further reasons for installing the FNLS (notably for HostID management), to the point where FNLS will inevitably become a required component for certificate-only applications.

Without the FNLS, the following virtualization behaviour will now occur on Windows

- SERVER line HostID keyword `VM_UUID` is not extracted: the vendor daemon will therefore shut down if this HostID is used when FNLS is not installed on the server.
- `lc_virtualstatusget` will return the pre-existing error code -1 instead of 0 (physical) or 1 (virtual).
- `lc_get_attr` (`LM_A_VM_FAMILY` or `LM_A_VM_NAME`) will return a null attribute string.
- The server log (SLOG) virtualization entry will report virtualization status as 'Not determined'.
- `ls_allow_vm` vendor variable: if the server does not have FNLS installed, the behaviour will be as if the server were on a physical platform.
- `VM_PLATFORMS` license file keyword – the license server will treat clients without FNLS installed as physical.

Note: `VM_PLATFORMS` and `ls_allow_vm` are first-generation virtualization 'detect-and-deny' features, which now have little value, and are candidates for deprecation.

In order to assist a license administrator to determine that the FNLS is now required for virtualization attribute extraction, `lmvminfo` and `lmhostid -ptype VM uuid` now both return the message "The FlexNet Licensing Service is not installed" when the FNLS is not installed.

Producers can generate such a message in their own applications, via the new `lc_fnpservice_present(lm_job)` API, which returns a non-zero positive integer if the FNLS is installed and startable (so not disabled), otherwise zero. One current limitation of the API is that it does not indicate if a too-old-to-use version of the FNLS is present. This API will support detection of the Linux FNLS in a future release, and may change to return richer information concerning the status and version of the FNLS via negative integer values.

License administrators administering certificate-only license servers that use virtualization features now need to install the FNLS. Additionally, when installing the license server as a Windows service, a start-permission DACL needs to be applied to the FNLS – this allows the license-server-service to start the FNLS. This can be done in `lmtools` by selecting the “Trusted storage in use” checkbox, which applies the DACL to a pre-installed FNLS. `lmadmin` applies the DACL automatically when installing itself as a service, provided FNLS has been pre-installed.

On Windows, the first-time checkout performance now approximates that of the FNP 11.8 release, if the FNLS is installed (FNP-14829).

Two other problem behaviours are improved through the above FNLS changes

1. Whilst OpenStack is not a supported environment, it does emulate the Amazon EC2 detection interface, by supporting connections to <http://169.254.169.254/latest/meta-data/>. The OpenStack implementation of this interface is however not optimal, meaning the node responsible for routing these requests can become overloaded if there are large numbers of processes making them (FNP-14830). Moving virtualization detection to the FNLS limits the number of metadata requests that originate from FNP-based applications running on a machine, improving this situation.
2. On Windows, in the presence of some anti-virus systems such as Kaspersky or AVG, queries to link-local addresses (169.254.*.*) can result in a WSACleanup delay. This manifested in FNP as a first-time checkout delay of up to 90 seconds. Now, if the FNLS is set to start automatically, this first-checkout delay is not seen from approximately two to three minutes after OS boot (FNP-14338).

Other Virtualization Resolved Issues

Inconsistent results from LM_A_VM_NAME and LM_A_VM_FAMILY

Previously, calling `lc_get_attr(LM_A_VM_NAME or LM_A_VM_FAMILY)` could produce inconsistent results. This was first seen when testing from a Windows VM on VMware ESXi, but could have manifested with other virtualization stacks (FNP-15111).

AMZN_EIP HostID

Support for `AMZN_EIP` on the `SERVER` line is reintroduced in this service pack (FNP-14827). However, a bug remains in Linux EC2 instances where running `lmreread` on a vendor daemon using `AMZN_EIP` HostID will cause a restart. Since there is no workaround, the recommendation is to limit use of `AMZN_EIP` to Windows instances until the bug is fixed (FNP-15137).

Note: For the time being `AMZN_EIP` remains supported without the FNLS.

Other FlexNet Licensing Service issues

Running the license server as a service and upgrading FNLS

If Imgrd or Imadmin is configured as a Windows service, and is dependent on FNLS, then one step involved in the configuration is to apply a DACL to the FNLS which provides permission for the license-server-as-a-service to start the FNLS. This is done transparently by Imadmin when installing itself as a service, or by Imtools when installing Imgrd as a service, if the “Trusted storage in use” checkbox is checked. Additionally, the installs.c sample provides sample code for applying the DACL. Previously, this DACL was lost when the FNLS was upgraded. For Imadmin, this manifested as a disappearance of previously available trusted storage licenses. Now, an upgrade of the FNLS via fnpActSvcInstallWin (as used in the installanchorservice utility) or fnpActSvcInstallForMSI will retain the DACL from the original FNLS (FNP-14837).

Known issue: Change in error code displayed when the FNLS is older than the FNP client

A version of FNLS greater than or equal to that of the FNP activation library (<vendor>_libFNP.dll) is required. If the FNLS is too old, calling flxActCommonLibraryInit or flxActCommonHandleOpen should cause the system error code LM_TSSE_SERVICE_TOO_OLD (10103, refer FlxActSystemError.h) to be set. In 11.14.0.1 this behaviour has regressed – these functions still fail, but this system error code is not set (FNP-15128). This will be resolved in a future release.

Certificate borrow resolved issues

The following borrow bugs exist in 11.14.0.0 and have been resolved in 11.14.0.1

- If two features are borrowable, and one feature name is a substring of the other, then one of the features may fail to return properly (FNP-14828), or one of the features may unexpectedly perform a borrow checkout when a normal concurrent checkout is expected (FNP-14824). Fix is client-side.
- Multiple borrows of a mix of borrowable features may cause extra count to be erroneously deducted from some features (FNP-15072, client-side fix).
- If a feature is borrowed, then returned, then the server restarted, then the same feature borrowed again, a second return may fail (FNP-14839, server-side fix)
- With 11.14.0.0 server, a client of an earlier version may fail a borrow return (FNP-14924, server-side fix).
- If PACKAGE components are borrowed, then returned, and the server restarted, the server will erroneously report the package feature as borrowed again (FNP-14823, server-side fix).

Windows Visual Studio 2015 compatibility

Previously, makefile and makefile.act would not build with the DEBUG=1 option when using Visual Studio 2015. This has now been resolved (FNP-14972).

Dongle updates

Legacy FLEXID9 HASP4 dongle support

(This item was mistakenly omitted from the FNP 11.14.0.0 release notes, so is included here).

In FNP 11.14.0.0, a client side attribute, `LM_A_FLEXID9_HASP4_SUPPORT`, and equivalent server-side attribute, `ls_flexid9_hasp4_support` – set in `lsvendor.c`, were introduced. By default, these attributes are set to 0 (off), meaning that FLEXID9 HostID is not by default extracted from legacy HASP4 dongles. These attributes were introduced to fix a FLEXID9 latency issue that occurs only with the legacy third-party API required for extracting the HostID from HASP4 dongles (FNP-11619). To continue supporting HASP4 dongles, producers should set these attribute values to 1, but Flexera's recommendation is that producers gradually replace HASP4 dongles with the newer HASP HL dongles.

Dongle driver update – FLEXID10 on Windows

Wibu dongle drivers have been updated from v6.30 to v6.32, only on Windows in this service pack (FNP-14826). No other dongle updates are delivered in this service pack.

Unfortunately, Windows FNP versions earlier than 11.14.0.1 will fail to extract FLEXID10 with v6.32 or later dongle drivers. This is because FNP verifies the code signature of the dll provided by Wibu, in order to prevent dll spoofing exploits. Part of that verification involves checking the base issuer of the certificate, which has changed from Verisign (v6.30 and earlier) to Symantec (v6.32 and later). Therefore, an upgrade of the Windows Wibu driver to v6.32 necessarily requires an upgrade of FNP, client or server (FNP-14848).

3-Server enhancement

Determining if a license server is master

The new API `ls_get_status_is_master`, declared in `ls_attr.h`, can be used from the vendor daemon's `ls_daemon_periodic` callback (and only from that callback) within `lsvendor.c` to determine if that vendor daemon is master. `ls_get_status_is_master` returns a non-zero integer if the vendor daemon is master (FNP-14843). The API cannot be called from `ls_user_initx` callbacks because this state is unknown at that point. A limitation is this API works only from vendor daemons started with `lmgrd`. All of a triad's vendor daemons started with `lmadmin` will report a non-zero value from `ls_get_status_is_master` (FNP-15005).

VCG enhancement

VCG and XFS filesystems

i86_ls VCG is now compatible with XFS filesystems (FNP-14971).

Note: The version of the VCG delivered with this service pack is 16.2.0.0.

Resolved certificate issues

Lmgrd and invalid license file extensions

Refer the lmadm note for FNP-14825 below.

License server Windows service paths may now contain spaces

Previously, when the license server was installed as a Windows service, the service path was not quoted. This meant that service paths containing spaces would not install correctly. Now, installs.exe, lmttools.exe and lmadm.exe all quote the service path (FNP-14867).

Signing expired licenses with lmcrypt

To allow producer testing of expired-license test cases, lmcrypt will now successfully sign a license file with an expired but otherwise valid license (FNP-14840)

Error codes returned by the license server to the client

Prior to 11.14.0.0, the license server returned a LM_NOSERVSUPP error to the client for expired or unserved features. In 11.14.0.0, this was changed so that the following pre-existing and more appropriate error codes are now received by the client.

- Feature not served: LM_NOFEATURE
- Feature expired: LM_LONGGONE
- Feature start date in future: LM_TOOEARLY

In 11.14.0.1, to cater for legacy clients that are coded directly to LM_NOSERVSUPP for the above error conditions, a *temporary* vendor variable, `ls_prefer_noservsupp` can now be set in `lsvendor.c`. If set to 1 (default value 0) the license server will return the prior error code LM_NOSERVSUPP in all the above scenarios. Note that `ls_prefer_noservsupp` will not be documented other than in this release note, and will not be supported beyond 2017.

Shutting down a single license server with lmttools when the license path specifies multiple license servers

If lmttools is used to configure the license server as a Windows service on two machines; and `VENDOR_LICENSE_FILE` is set to include both license servers; and lmttools is used to shut down one of the servers, then the second license could previously be inappropriately shut down. This has been resolved (FNP-14854).

Lmttools display of system information

Lmttools will now display both IPv4 and IPv6 address, if available (FNP-14832). CPUID and disk volume serial number are no longer displayed, since they now have no licensing value (FNP-14833).

Java kit resolved issue

Supplying a directory as a license source works once again, as evidenced by running a command like `java BasicExample fl 1.0 "<license file folder>"` (FNP-14838)

Lmadm resolved issues

All lmadm changes in this service pack are security vulnerability resolutions.

Uploading or importing potentially malicious license files

This issue was originally raised as “uploading batch files as license files” (FNP-14825). Previously, it was possible to have lmadm import a potentially malicious license file (such as one with a .bat extension on Windows) that could separately be run by an adversarial user after being imported. Additionally, in the case of Windows, the act of opening a batch file runs the file, meaning that the Windows vendor daemon could also inadvertently run the batch file masquerading as a license file. Whilst the impact of this is limited, since the vendor daemon runs at user-level privilege, the following behaviour changes have been made:

On Windows: lmadm will perform file extension checks on license files it imports. The following extensions (checked with case insensitivity) are first checked in a whitelist: ‘.dat’, ‘.lic’ and ‘.txt’. Extensions not found in the whitelist but found in a blacklist (containing ‘.bat’ amongst other disallowed extensions) will fail to import with an “Invalid License File” message. Best-practice for producers is to enforce use of whitelisted extensions for license files.

On non-Windows: lmadm will check for execute permission on the license file. If execute-permission is found, and lmadm fails to remove the execute permission, the license file will fail import.

Neither the whitelist nor the blacklist is configurable.

For consistency, lmgrd will follow similar behaviour, using the same white and blacklists as lmadm. For example, a command such as `lmgrd -c counted.bat` (on Windows) will result in a “Cannot find license file” message in the server log. On non-Windows, this is allowed provided there is no execute permission on counted.bat, or the execute permission can be removed by lmgrd.

Other resolved lmadm security vulnerabilities

A DoS vulnerability via a specially crafted message to lmadm was resolved (FNP-14553).

lmadm help html is no longer cacheable (FNP-14836).

Cookies sent by lmadm over SSL now have the secure attribute set (FNP-14835).

Trusted Storage resolved issues

Lmstat reporting of licenses signed with legacy license keys

Previously, if multiple fulfillments using the same ActivationID were activated to server trusted storage, and each fulfillment's INCREMENT lines were signed with legacy license keys, then Lmstat would report an incorrect count for those features. A fix for Lmgrd based license servers, but not for Lmadmin based license servers, has been delivered (FNP-14379). This issue will not be fixed for Lmadmin. Producers are reminded that license keys are weak signatures and are deprecated.

Cancelling a pending shortcode request

Previously, an attempt to cancel a pending shortcode request via a command such as `./appcomptranutil -shortcode publisher/xml/ShortCode2016High.asr -cs` would terminate without success. This has now been resolved in the comptranutil sample utilities (FNP-14339).

Short codes with the high response signing strength option

On some Linux machines the processing of a response using high signing strength short code ASRs did not verify a valid response signature, generating a 50058 error. This has now been resolved (FNP-14533).

Supported Platforms

Service Pack 2 delivers the following subset of FlexNet Publisher archives: i86_n3, x64_n6, i86_lsb, x64_lsb, universal_mac10_applelicpp, x86_sol9, x64_sun10, sun4_u10 and sun64_u9. For more platform details, see FlexNet Publisher 2016 R1 (11.14.0) release notes. Refer to <http://www.flexerasoftware.com/support/eol/flexnet-publisher-end-of-life.htm> for the latest information on supported platforms.

Legal Information

Copyright Notice

Copyright © 2016 Flexera Software LLC. All Rights Reserved.

This publication contains proprietary and confidential information and creative works owned by Flexera Software LLC and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera Software LLC is strictly prohibited. Except where expressly provided by Flexera Software LLC in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera Software LLC intellectual property rights, whether by estoppel, implication, or otherwise. All copies of the technology and related information, if allowed by Flexera Software LLC, must display this notice of copyright and ownership in full.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera Software, see <http://www.flexerasoftware.com/intellectual-property/>. All other brand and product names mentioned in Flexera Software products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.